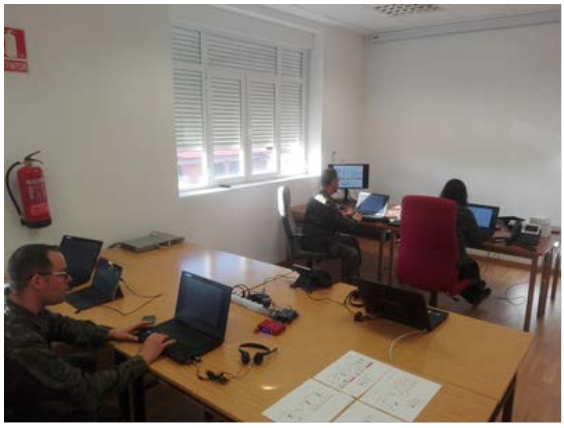
Boletín informativo del Departamento de Productos y Tecnologías de Seguridad TIC del Centro Criptológico Nacional (CCN-PYTEC).

Boletín CCN-PYTEC nº14 - 02/2019

Comunicaciones Tácticas Seguras

JCISAT y CCN experimentan escenarios Wi-Fi seguro para la BRIEX (Brigada Experimental) 2035 (01/2019).



Durante la última semana de enero, en el Acuartelamiento Capitán Sevillano, personal de la Sección de Arquitectura e Interoperabilidad (SECARQINT) de JCISAT/SUBCIS del Ejército de Tierra y del CCN probaron una serie de escenarios Wi-Fi considerando tres dominios de seguridad diferenciados, que reproducen los entornos de seguridad que se establecerían en un Puesto de Mando de Brigada:

- RESERVADO (RES),
- DIFUSIÓN LIMITADA (DL) y
- SIN CLASIFICAR (SC)

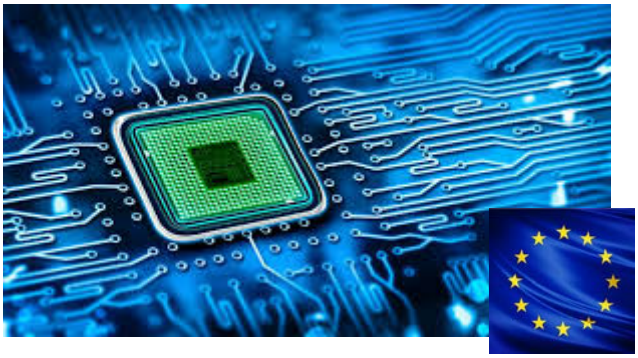
Para la protección de la confidencialidad de la información se emplearon productos de cifra *software* (para DL) y *hardware* (para RES) recomendados por el CCN (productos actualmente en evaluación y que se prevé sean aprobados en el futuro).

Estas pruebas demostraron la viabilidad de emplear de forma segura tecnologías inalámbricas que faciliten el despliegue rápido de puestos de mando, tanto de nivel Brigada como de nivel Batallón y permitió detectar una serie de incidencias, que se prevé subsanar en los próximos meses cuando, además, se llevarán a cabo pruebas adicionales con nuevas infraestructuras inalámbricas, tanto WiFi como LTE. Posteriormente, se prevé realizar una validación operativa de las soluciones por parte de la Brigada Experimental de La Legión.

Esta iniciativa se enmarca dentro de los experimentos que se están desarrollando en el marco BRIEX 2035, a través del cual el Ejército de Tierra evalúa productos y tecnologías que sirvan para desarrollar su nuevo concepto de Brigada del futuro, conocido como Brigada 2035.

Tecnología para seguridad

El CCN colaborará en el proyecto para el prototipado de un SoC europeo (01/2019).



Dentro de la convocatoria de la Acción Preparatoria sobre Investigación en Defensa, lanzada por la EDA para el año 2018, se propuso el proyecto "*European high-performance, trustable, (re)configurable system-on-a-chip for defence applications*". Este proyecto pretende impulsar la investigación en tecnologías SoC (*System on Chip*), empleadas en numerosos equipos para defensa, y particularmente en muchos productos de cifra. El CCN considera este proyecto de gran interés ya que actualmente este tipo de tecnologías son manufacturadas fuera de la UE, lo que implica un riesgo en cuanto a posibles vulnerabilidades de seguridad introducidas durante el proceso de fabricación. Dentro del alcance del proyecto se desarrollará un prototipo de SoC que deberá cumplir con los requisitos de la UE exigibles a los productos de cifra de nivel de seguridad muy alto. El CCN y organizaciones equivalentes (NCSAs) de otros estados miembros participarán en un *Advisory Board* que supervisará el desarrollo de las actividades y el cumplimiento de los requisitos.

Productos STIC

La certificación LINCE, herramienta para inclusión en el CPSTIC (02/2019).

La Certificación Nacional Esencial de Seguridad, conocida como LINCE, incluye una metodología orientada a la evaluación y certificación de productos de seguridad TIC para su inclusión en el CPSTIC (CCN-STIC-105) como productos cualificados para ENS Medio y Bajo. Excepcionalmente, cuando no existan productos de categoría ENS Alto para una familia determinada, la certificación LINCE también podría ser suficiente para la inclusión en este nivel (normalmente se requiere una certificación Common Criteria). La metodología LINCE también se puede emplear para la realización de evaluaciones STIC complementarias conforme a lo especificado en la CCN-STIC-106 y CCN-STIC-140. LINCE se está conviertiendo en un mecanismo demandado por los fabricantes para la inclusión de sus productos en el Catálogo de Productos STIC del CCN. De hecho, la creciente demanda ha provocado que hasta siete laboratorios del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información se estén acreditando en esta metodología.

Comunicaciones Móviles Seguras

Samsung Galaxy S9, cualificado para ENS Alto (02/2019).

Samsung Galaxy S9 entra en el Catálogo de Productos de Seguridad TIC como cualificado para ENS Alto, tras la realización de las correspondientes pruebas de evaluación por parte del CCN. Este *smartphone* destaca por su pantalla infinita, su avanzada cámara y por contar con la certificación IP68. La plataforma de seguridad Samsung Knox está integrada en el *hardware* y operativa desde que se enciende el dispositivo. Dispone de una memoria de almacenamiento de 64 GB ampliables mediante microSD hasta 512GB más. El CCN publicará proximamente una guía CCN-STIC de configuración segura para este dispositivo, de manera que las organizaciones puedan desplegarlo de la manera correcta y utilizar todas las funcionalidades de Samsung Knox.

EMSEC

Actualizado el Catálogo de Productos con clasificación ZONING, (01/2019).

Se ha procedido a la actualización de la guía CCN-STIC-104 "Catálogo de Productos con clasificación ZONING" en el mes de enero 2019. Se han incluido nuevos equipos y sistemas evaluados en los últimos meses. Este catálogo facilita la selección de equipamiento informático que pueda cumplir con una determinada clasificación ZONING. Es de aplicación para equipos que deban manejar información clasificada NATO CONFIDENTIAL/EU CONFIDENTIAL/CONFIDENCIAL, o superior, y vayan a ser instalados en locales con clasificación ZONING de ZONA 1 o superior.

Common Criteria / Cripto

El CCN en el Crypto Working Group de SOGIS (01/2019).

Especialistas criptólogos y de Common Criteria del Organismo de Certificación del CCN han participado en la última reunión del Crypto Working Group. El principal cometido de este grupo de trabajo, es acordar la criptografía de referencia en el ámbito del SOGIS MRA, establecer una metodología de evaluación para dicha criptografía y proporcionar los mecanismos necesarios para armonizar la aplicación de dicha metodología por parte de los diferentes Esquemas de evaluación y certificación europeos. Todo ello con el objetivo de poder certificar la criptología de un producto de seguridad y que esa certificación sea reconocida por todos los Esquemas europeos miembros del SOGIS-MRA.

Eventos

CCN-PYTEC asiste a la reunión de la Allied Crypto Task Force (01/2019).

Entre los días 22 y 25 de enero se celebró en Roma la 11ª Reunión del Grupo de trabajo Cripto de la Alianza (*Allied Crypto Task Force*, ACTF). En este grupo de trabajo, dependiente del Comité Militar de la Alianza, se exponen la situación operacional de las redes que utilizan equipamiento cripto y la evolución futura de los medios de cifra en función de las necesidades de la OTAN como organismo y la de los distintos países que la integran. Dentro del ámbito de este grupo de trabajo se está coordinando la sustitución de equipamiento cripto obsoleto en las redes de comunicaciones de la OTAN y el desarrollo de programas de adquisición de nuevas capacidades criptológicas que garanticen la seguridad de las comunicaciones operativas. Así mismo se ha abierto una nueva línea de actuación para la definición de una estrategia y las medidas técnicas y operacionales necesarias para prevenir la amenaza de un procesador cuántico criptológicamente relevante.

El CCN, presente en la MPC de CWIX 2019 (02/2019).

El CCN asistió a la *Main Planning Conference* (MPC) de CWIX 2019, celebrada en la localidad danesa de Slagelse entre los días 29 de enero y 1 de febrero. La participación del CCN dentro del área de interés de comunicaciones se centró en la planificación de las pruebas de interoperabilidad de productos de cifra de diferentes naciones OTAN que implementan las especificaciones criptográficas NINE (STANAG 4787), SCIP (STANAG 5068) y STaC-IS (anexo del STANAG 5068). Hasta la fecha se han planeado pruebas de interoperabilidad criptográfica entre productos de diferentes fabricantes polacos, italianos, noruegos y españoles. Además, también se ha identificado la oportunidad de probar algunos de estos productos junto con formas de onda para interoperabilidad radio (ESSOR HDRWF, NATO NBWF…) y routers tácticos (GESCOMET y otros).

Contacto

Correo electrónico CCN-PYTEC	ccn-pytec@cni.es
Twitter	**@CCNPYTEC**
LinkedIn	**https://www.linkedin.com/company/CCN-PYTEC**